

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号  
特開2002-353958  
(P2002-353958A)

(43)公開日 平成14年12月6日(2002.12.6)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	データコード*(参考)
H 0 4 L 9/32		B 4 2 D 15/10	5 0 1 E 2 C 0 0 5
B 4 2 D 15/10	5 0 1		5 1 1 5 B 0 8 5
	5 1 1		5 2 1 5 J 1 0 4
	5 2 1	G 0 6 F 15/00	3 3 0 B
G 0 6 F 15/00	3 3 0	17/60	2 2 2
審査請求 未請求 請求項の数24 O L (全 17 頁) 最終頁に続く			

(21)出願番号 特願2001-153854(P2001-153854)

(22)出願日 平成13年5月23日(2001.5.23)

(71)出願人 598049322

株式会社東京三菱銀行  
東京都千代田区丸の内2丁目7番1号

(72)発明者 飯坂 俊治

東京都千代田区丸の内2丁目7番1号 株  
式会社東京三菱銀行内

(74)代理人 100086863

弁理士 佐藤 英世

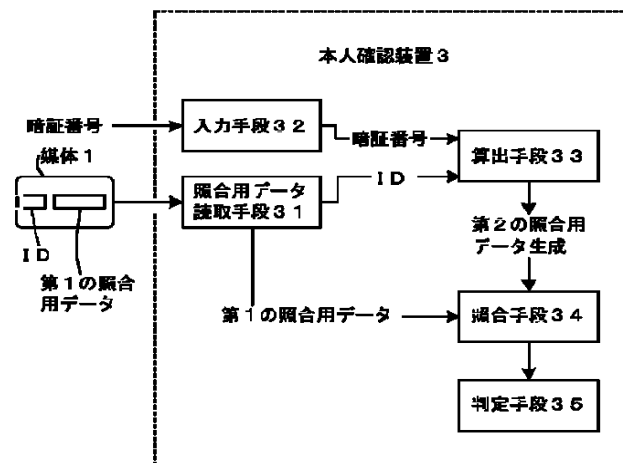
最終頁に続く

(54)【発明の名称】 本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体

(57)【要約】

【課題】 他の装置との接続が要求されることなく媒体単体で本人確認が完結でき、しかも本人確認のために入力される情報を媒体上にそのまま格納せずに、正確な本人確認が行える本人確認方法を提供せんとするものである。

【解決手段】 ユーザIDと暗証番号のデータ列に対してハッシュ関数により処理して得られる第1の照合用データ及び上記ユーザIDの記録された媒体1から、第1の照合用データ及びユーザIDが読み取られると共に、読み取られたユーザIDと入力された暗証番号のデータ列に対して上記と同じハッシュ関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われる。



## 【特許請求の範囲】

【請求項1】 少なくとも暗証データに対して一方向性関数により処理して得られる第1の照合用データの記録された媒体から、コンピュータ上に第1の照合用データが読み取られると共に、入力された暗証データに対し上記と同じ一方向性関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われることを特徴とする本人確認方法。

【請求項2】 ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、コンピュータ上に第1の照合用データ及びユーザデータが読み取られると共に、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われることを特徴とする本人確認方法。

【請求項3】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものをを用いることを特徴とする請求項1又は請求項2記載の本人確認方法。

【請求項4】 少なくとも暗証データに対して一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データを読み取る照合用データ読み取り手段と、暗証データの入力手段と、入力された暗証データに対して上記と同じ一方向性関数によって第2の照合用データを算出する算出手段と、上記第2の照合用データと前記第1の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴とする本人確認装置。

【請求項5】 ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータを読み取る照合用データ読み取り手段と、暗証データの入力手段と、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第2の照合用データを算出する算出手段と、上記第2の照合用データと前記第1の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴とする本人確認装置。

【請求項6】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものをを用いることを特徴とする請求項4又は請求項5記載の本人確認装置。

【請求項7】 少なくとも暗証データが与えられることにより一方向性関数により処理して第1の照合用データを算出する演算手段と、該第1の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴とする媒体作成装置。

【請求項8】 ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列が与えられることにより一方向性関数により処理して第1の照合用データを算出する演算手段と、

該第1の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴とする媒体作成装置。

【請求項9】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものをを用いることを特徴とする請求項7又は請求項8記載の媒体作成装置。

【請求項10】 暗証データに対して一方向性関数により処理して得られる第1の照合用データを格納するための領域を有することを特徴とする媒体。

【請求項11】 ユニークなユーザデータと暗証データを構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データを格納するための領域を有することを特徴とする媒体。

【請求項12】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものをを用いることを特徴とする請求項10又は請求項11記載の媒体。

【請求項13】 少なくとも暗証データに対して第1の一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データが読み取られ、入力された暗証データに対し上記第1の一方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上に第1の照合用データ、第3の照合用データ及び上記保管情報が読み取られるステップと、別途入力された暗証データに対し上記第1の一方向性関数によって第4の照合用データが算出されるステップと、第4の照合用データと読み取られた前記第1の照合用データとが照合されるステップと、

読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データが算出されるステップと、  
上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとが照合されるステップと、  
第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを  
実行することを特徴とする媒体保管情報の処理方法。

【請求項14】 ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上にユーザデータ、第1の照合用データ、第3の照合用データ及び上記保管情報が読み取られるステップと、  
別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第4の照合用データが算出されるステップと、  
第4の照合用データと読み取られた前記第1の照合用データとが照合されるステップと、  
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データが算出されるステップと、  
上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとが照合されるステップと、  
第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを  
実行することを特徴とする媒体保管情報の処理方法。

【請求項15】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを  
用いることを特徴とする請求項13又は請求項14記載の媒体保管情報の処理方法。

【請求項16】 少なくとも暗証データに対して第1の一方方向性関数により処理して得られる第1の照合用データを格納するための第1の格納領域と、  
該格納領域に第1の照合用データの記録された状態から、該照合用データが読み取られ、入力された暗証データに対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致した場合に格納される、該保管情報のための第2の格納領域と第3の照合用データのための第3の格納領域とを有することを特徴とする媒体。

【請求項17】 ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方方向性関数により処理して得られる第1の照合用データを格納するための第1の格納領域と、  
上記ユーザデータを格納するための第2の格納領域と、  
これらの格納領域に第1の照合用データ及びユーザデータの記録された状態から、第1の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致した場合に格納される、該保管情報のための第3の格納領域と第3の照合用データのための第4の格納領域とを有することを特徴とする媒体。

【請求項18】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものを  
用いることを特徴とする請求項16又は請求項17記載の媒体。

【請求項19】 コンピュータに、  
少なくとも暗証データに対して一方方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データを読み取らせるステップと、  
入力された暗証データに対し上記と同じ一方方向性関数によって第2の照合用データを算出させるステップと、  
該第2の照合用データと前記第1の照合用データとを照合させ、本人確認を行うステップとを実行させることを  
特徴とするプログラム。

【請求項20】 コンピュータに、  
ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方方向性関数により処理し

て得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータを読み取らせるステップと、  
読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ方向性関数によって第2の照合用データを算出させるステップと、  
該第2の照合用データと前記第1の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴とするプログラム。

【請求項21】 コンピュータに、  
少なくとも暗証データに対して第1の一方方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データが読み取られ、入力された暗証データに対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記記体から、第1の照合用データ、第3の照合用データ及び上記保管情報を読み取らせるステップと、  
別途入力された暗証データに対し上記第1の一方方向性関数によって第4の照合用データを算出させるステップと、  
第4の照合用データと読み取られた前記第1の照合用データとを照合させるステップと、  
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データを算出させるステップと、  
上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとを照合させるステップと、  
第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴とするプログラム。

【請求項22】 コンピュータに、  
ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータが読み取られ、入力された暗証データ及び上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照

合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、ユーザデータ、第1の照合用データ、第3の照合用データ及び上記保管情報を読み取らせるステップと、  
別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第4の照合用データを算出させるステップと、  
第4の照合用データと読み取られた前記第1の照合用データとを照合させるステップと、  
読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データを算出させるステップと、  
上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとを照合させるステップと、  
第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴とするプログラム。

【請求項23】 前記暗証データは、外部から感知できるユーザの特徴を検出し、任意のデータに変換したものをを用いることを特徴とする請求項19～請求項22いずれか1つに記載のプログラム。

【請求項24】 請求項19～請求項23のいずれかのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、セキュリティを高めた本人確認方法、本人確認装置、媒体作成装置、該媒体作成装置で作成され前記本人確認装置に用いられる媒体、その媒体に保管された情報の処理方法、これらのプログラム及び記録媒体に関する。

【0002】

【従来の技術】これまでの本人確認方法の1つとして、磁気カードやICカードなどの媒体を使用するものがある。このような構成の場合は、媒体の所有者によって、この媒体に関連する特定の情報が入力されることで行われる。

【0003】上記本人確認の際入力される情報には、ユニークな（2つと無い）ユーザIDや暗証番号などがあり、通常これらの情報は、媒体中にも格納され、本人確認の都度、該媒体中から読み出されて、入力される情報

との突き合わせ処理が実施される。

【0004】すなわち金融機関などと取引を行うサービスで利用される媒体には、磁気カードやICカードなどが使用されている。そのうち①キャッシュカード・デビットカードなどの媒体による取引では、媒体の所有者（口座保有者）が、ATM、POS端末等で機器操作を行う場合、本人のみが知る暗証番号（通常4桁の数字）を機器に対して入力する。機器はカードより読み取った「データ」及び入力された「暗証番号」を1つの電文として送信し、発行体のホストコンピュータにおいて、入力された暗証番号が登録されたものと同一かどうかを照合し、本人確認を行う。

【0005】また②ICカードなどを使用するICクレジット取引・電子マネー取引等では、利用者がICクレジットカードを利用する都度、或いは電子マネー等を使って「小額な」支払いをする都度、入力された暗証番号と、ICカードに登録された「暗証番号」とをICチップ上で照合し、ホストに接続することなく、本人確認を行うスキームが存在する。この場合、利用ごとにホストコンピュータに接続しない（オフライン処理）ため、通信料金、データ処理料金等のコストが節減できる。

【0006】

【発明が解決しようとする課題】ところが、媒体中にこのような暗証番号などの情報が格納されていると、これらの情報解析を行うハッキング技術の標的になる場合が多い。このようなことは、磁気カードばかりか、一般に解析が難しいとされる上記ICカードなどの媒体でも同じである。

【0007】これに対し、セキュリティを高めるために、以上の情報のうち暗証番号については、媒体への格納が行われず、特定の装置と接続された際に、該暗証番号の入力が要求され、オンラインで本人確認がなされるようにすることも考えられる。

【0008】しかし、本人確認の際に常に特定の装置との接続が要求されるとなると、利用者側に余計な負荷がかかるなど、使い勝手が悪くなる。特にICカードなどに特定の金銭的価値を有するデータを格納させて電子通貨として使用する場合、支払の都度、特定のサーバへの接続が行われて、本人確認が実施されるようにしたのは、電子通貨の利便性が損なわれることにもなりかねない。また特定のサーバへのトラフィックが増大し、各処理の本人確認が終了するまでに時間がかかってしまうことも想定される。

【0009】他方、「J A V A（登録商標）カード」、「MULTOSカード」、或いは「スマートカード for WINDOWS（登録商標）」などの汎用OSカードと呼ばれるカードは、後からソフトウェアなどの情報をカード上に書き込み・格納できる機能を有している。その場合にそれらの情報を書き込める者を確認する必要があるが、そのような情報の書き込みは、権限を与

えられた特定のソフトウェアができるのみで、「権限の与えられた人間」ができるというものではない。ましてや書き込まれた情報を利用しようとする人物が、カードなどの媒体の正しい所有者乃至該媒体に情報を記録した者であるなどといった照合が行われたり、その内容に改竄がないなどの確認がなされることは保証されていない。

【0010】本発明は、以上のような問題に鑑み創案されたもので、他の装置との接続が要求されることなく媒体単体で本人確認が完結でき、しかも本人確認のために入力される情報を媒体上にそのまま格納せずに、正確な本人確認が行える本人確認方法、本人確認装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体を提供せんとするものである。

【0011】また媒体上に任意の情報が書き込まれてそれが利用できる構成において、書き込まれた情報を利用しようとする人物が、媒体の正しい所有者乃至該媒体に情報を記録した者であるなどといった照合ができ、しかもその内容に改竄がないなどの確認ができるような構成についても、併せて提案せんとするものである。

【0012】

【課題を解決するための手段】本発明は、少なくとも暗証データに対して、ハッシュ関数などの一方向性関数（処理結果から元データを割り出すことができない或いは難しい関数）により処理して得られる第1の照合用データの記録された媒体から、コンピュータ上に第1の照合用データが読み取られると共に、入力された暗証データに対し上記と同じ一方向性関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われることを基本的特徴としている。

【0013】上記構成によれば、媒体中に格納されるデータは、暗証番号などの暗証データそのものではなく、一方向性関数により処理して得られる第1の照合用データであり、そのため、仮に媒体からこれらのデータが読み出せたとして、第1の照合用データからは、暗証データを割り出す（推測する）ことはできない。従って本人確認の際に暗証データの入力を要求することで、入力された暗証データに対し上記と同一の一方向性関数で処理し、その結果得られた第2の照合用データと、前記媒体より読み取った第1の照合用データとの突き合わせを行い、その照合結果で本人確認処理を行えば、他の装置との接続が要求されることなく媒体単体で本人確認が完結できることになる。また媒体上に格納されるデータは、本人確認のために入力される情報そのものではなく、しかも媒体上に格納されるデータからは、上記入力の要求されるデータの割り出しが困難なため、セキュリティも向上することになる。すなわち、ユーザ以外は、いかなる者も真の暗証データを目にすることなく安全に媒体が作成され、媒体の盗難、偽造などに対しても、極めて強

力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体作成中の暗証データの盗難リスクなども回避されるようになる。

【0014】請求項2の構成は、さらに両照合用データの生成に当たり、他人の者との一致を排除する構成である。すなわち、暗証データは、通常ユーザ側が自由に選択・決定するため、ユーザ間で同じものを選択してしまう確率は全くないとは言えず、従って照合用データも個々のユーザにユニークなものになるとは限らない。そこで、ユーザ側に選択権のない（或いはユーザ側の選択権が限られる）、各ユーザ毎にユニークな状態で割り当てられるユーザIDなどのユーザデータを照合用データの生成に利用することにした。

【0015】具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、コンピュータ上に第1の照合用データ及びユーザデータが読み取られると共に、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第2の照合用データが算出され、該第2の照合用データと前記第1の照合用データとが照合されることで、本人確認が行われることを特徴としている。

【0016】上記ユーザデータと暗証データは、一方を他方の後に一連につなげて使用する場合は、両データを互いに加減乗除して使用したり、或いは適当な数字で加減乗除しその後一連につなげて使用したりするなど、両データを使用することで、照合用データの生成前にユニークなデータとして得られるものであれば、これらのデータの用いられ方には、特に限定はない。

【0017】上記請求項1、請求項2の構成において、使用される媒体に記録されているものは、第1の照合用データであり、上述のように解析することはできないが、暗証データが盗用された場合は、上記媒体乃至そのコピー品を使用する限り、本人と誤認識されてしまう可能性がある。そのようなことを想定した場合、該媒体に記載される暗証データは、外部から感知できるユーザの特徴を何らかの形で検出し、任意のデータに変換したものをを用いる方が良い。すなわち、ユーザに記憶されるものではなく、例えばユーザの身体的特徴（指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報）を検出し、その検出データを使用すれば、ユーザは暗証データを覚える必要が無くなって、単に検出機器にその身体部分を検出させれば良く、そのために他人による暗証データの盗用はできなくなるため、セキュリティレベルは非常に高度のものとなる（ハッキングによるなりすましは不可能となる）。これは、以下に示す他の請求項についても同様である（請求項3、6、9、12、1

5、18及び23）。

【0018】請求項4の構成は、上記請求項1の本人確認方法の構成を、本人確認を行う装置の構成として捉え直して規定したものであり、より具体的な構成としては、少なくとも暗証データに対して一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データを読み取る照合用データ読み取り手段と、暗証データの入力手段と、入力された暗証データに対して上記と同じ一方向性関数によって第2の照合用データを算出する算出手段と、上記第2の照合用データと前記第1の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴としている。

【0019】請求項7の構成は、上記本人確認装置で使用する媒体の作成装置を規定するものであり、具体的には、少なくとも暗証データが与えられることにより一方向性関数により処理して第1の照合用データを算出する演算手段と、該第1の照合用データを媒体に書き込む照合用データ書き込み手段とを有することを特徴としている。

【0020】請求項10の構成は、上記請求項1の方法乃至請求項4の装置で使用可能な媒体の構成を規定したものであり、より具体的には、暗証データに対して一方向性関数により処理して得られる第1の照合用データを格納するための領域を有する媒体である。なお、このような媒体としては、磁気記録カード、ICカード、光磁気カードなどがあり、データを記録できるものであれば、記録形式、媒体形状などの如何に拘わらず、用いることができる。

【0021】請求項5の構成は、上記請求項2の本人確認方法の構成を、本人確認を行う装置の構成として捉え直して規定したものであり、より具体的な構成としては、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータを読み取る照合用データ読み取り手段と、暗証データの入力手段と、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第2の照合用データを算出する算出手段と、上記第2の照合用データと前記第1の照合用データとを照合する照合手段と、上記照合結果に基づき、本人か否かの判定を行う判定手段とを有することを特徴としている。

【0022】請求項8の構成は、上記本人確認装置で使用する媒体の作成装置を規定するものであり、具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列が与えられることにより一方向性関数により処理して第1の照合用データを算出する演算手段と、該第1の照合用データを媒体に書き込む照

合用データ書き込み手段とを有することを特徴としている。

【0023】請求項11の構成は、上記請求項2の方法乃至請求項5の装置で使用可能な媒体の構成を規定したものであり、より具体的には、ユニークなユーザデータと暗証データを構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データを格納するための領域を有する媒体である。

【0024】一方請求項13の構成は、上記本人確認がなされた際、媒体中にユーザが任意の情報を記録する（保管情報の記録）と共に、それ以後、この保管情報の記録された媒体から、該保管情報を取り出して利用しようとする場合に、その利用をしようとする者が媒体の正しい所有者又は媒体に上記保管情報を記録した者であることの照合と記録された保管情報に改竄がないことの確認が行えるようにする構成を提供せんとするものである。

【0025】すなわち、請求項13に係る媒体保管情報の処理方法の構成は、少なくとも暗証データに対して第1の一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データが読み取られ、入力された暗証データに対し上記第1の一方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上に第1の照合用データ、第3の照合用データ及び上記保管情報が読み取られるステップと、別途入力された暗証データに対し上記第1の一方向性関数によって第4の照合用データが算出されるステップと、第4の照合用データと読み取られた前記第1の照合用データとが照合されるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第5の照合用データが算出されるステップと、上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとが照合されるステップと、第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することを特徴としている。

【0026】上記構成では、ユーザ側で任意の保管情報（例えばユーザの作成したソフトウェアやマクロ、機器操作情報、個人取引情報振込カード情報など）が記録された媒体が対象とされる。そのため、ユーザ側で保管情

報の記録操作を、下記のようにして行うことになる。

【0027】まず、ユーザは、少なくとも暗証データに対して第1の一方向性関数により処理して得られる第1の照合用データの記録された媒体を提供し、そこから、コンピュータ上に第1の照合用データを読み取らせる。一方ユーザは、コンピュータから暗証データの入力を要求され、これを入力する。ユーザがこれを入力した場合、該暗証データに対して上記第1の一方向性関数によって第2の照合用データが算出され、第2の照合用データと前記第1の照合用データとが照合される。他方入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第3の照合用データが算出される。そして、第2の照合用データと第1の照合用データとの照合でこれらのデータが一致した場合、前記保管情報と第3の照合用データとが、コンピュータによって、上記媒体に記録される。

【0028】すなわち、保管情報の媒体への記録に当たって、第1の照合用データと第2の照合用データとが照合されることで、本人確認を行い、媒体の正しい所有者のみが、媒体に上記保管情報の記録を行えることになる。

【0029】このような媒体から上記保管情報を読み出して、該保管情報の処理を行う場合にも、次のようにして、記録された保管情報の利用者が、媒体の正しい所有者乃至該媒体への保管情報記録者であるという照合と、記録された保管情報に改竄がないことの確認を行うことになる。

【0030】まず、ユーザは上記媒体を提供し、該媒体から、他のコンピュータ上に第1の照合用データ、第3の照合用データ及び上記保管情報を読み取らせる。またユーザは別途暗証データの入力を要求されるが、これに呼応して暗証データの入力を該コンピュータに対して行うと、該暗証データに対し上記第1の一方向性関数によって第4の照合用データが算出され、第4の照合用データと読み取られた前記第1の照合用データとが照合される。他方読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第5の照合用データが算出される。そして上記照合の結果、第4の照合用データと第1の照合用データとが一致した場合（記録された保管情報の利用者が、媒体の正しい所有者乃至該媒体への保管情報記録者であるという本人確認がされた場合）、読み取られた前記第3の照合用データと上記第5の照合用データとが照合される。第3の照合用データと第5の照合用データとが一致する場合は、保管情報の改竄がないと判断でき、読み取られた保管情報を、該コンピュータ上で処理することになる。

【0031】請求項16の構成は、上記媒体保管情報の処理方法で使用される媒体について規定しており、具体

的には、少なくとも暗証データに対して第1の一方方向性関数により処理して得られる第1の照合用データを格納するための第1の格納領域と、該格納領域に第1の照合用データの記録された状態から、該照合用データが読み取られ、入力された暗証データに対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致した場合に格納される、該保管情報ための第2の格納領域と第3の照合用データのための第3の格納領域とを有する媒体である。

【0032】請求項14の構成は、請求項2と同様、照合用データの生成に当たり、他人の者との一致を排除する構成である。すなわち、暗証データの他に、各ユーザ毎にユニークな状態で割り当てられるユーザデータも照合用データの生成に利用する。より具体的な構成としては、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、コンピュータ上にユーザデータ、第1の照合用データ、第3の照合用データ及び上記保管情報が読み取られるステップと、別途入力された暗証データ及び読み取られた上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第4の照合用データが算出されるステップと、第4の照合用データと読み取られた前記第1の照合用データとが照合されるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データが算出されるステップと、上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとが照合されるステップと、第3の照合用データと第5の

照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行することの特徴としている。

【0033】請求項17の構成は、上記媒体保管情報の処理方法で使用される媒体について規定しており、具体的には、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方方向性関数により処理して得られる第1の照合用データを格納するための第1の格納領域と、上記ユーザデータを格納するための第2の格納領域と、これらの格納領域に第1の照合用データ及びユーザデータの記録された状態から、第1の照合用データ及びユーザデータが読み取られ、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致した場合に格納される、該保管情報ための第3の格納領域と第3の照合用データのための第4の格納領域とを有する媒体である。

【0034】請求項19～請求項22までの構成は、請求項1及び請求項2に記載の構成並びに請求項13及び請求項14に記載の構成を、コンピュータで実行させるための、該コンピュータで実行可能なプログラムを規定している。すなわち、上述した課題を解決するための構成として、上記各ステップを、コンピュータの構成を利用することで実行する、該コンピュータで読み込まれて実行可能なプログラムを開示する。この場合、コンピュータとは中央演算処理装置の構成を含んだ汎用的なコンピュータの構成の他、特定の処理に向けられた専用機などを含むものであっても良く、中央演算処理装置の構成を伴うものであれば特に限定はない。

【0035】コンピュータに上記各ステップを実行させるための以下に示すプログラムが該コンピュータに読み出されて実行されると、請求項1及び請求項2に記載の構成並びに請求項13及び請求項14の構成に規定された各ステップと同様なステップが実行されることになる。

【0036】上記プログラムは、それ自身使用の対象となる他、後述のように記録媒体に記録されて配布乃至販売され、また通信などにより送信されて、譲渡の対象とすることもできるようになる。

【0037】尚、請求項19～請求項22記載の各ステップのうち一部の機能は、コンピュータに組み込まれた機能（コンピュータにハードウェア的に組み込まれている機能でも良く、該コンピュータに組み込まれているオ

ペレーティングシステムや他のアプリケーションプログラムなどによって実現される機能でも良い) によって実現され、前記プログラムには、該コンピュータによって達成されるこれらの機能と呼び出すあるいはリンクさせる命令が含まれるだけの構成であったとしても、本発明に規定する構成に含まれることは言うまでもない。

【0038】これは、請求項1及び請求項2に記載の構成並びに請求項13及び請求項14の構成に規定された各ステップの一部が、例えばオペレーティングシステムなどによって達成される機能の一部で代行され、上記プログラムにはその機能を実現するためのモジュールなどが直接記録されているわけではないが、それらの機能を達成するオペレーティングシステムの機能の一部を、呼び出したりリンクさせるようにしてあれば、実質的に同じ構成となるからである。

【0039】またこれらのプログラムが記録媒体に固定される(請求項24)ことで、これをソフトウェア商品として容易に配布、販売することができるようになる。また、既存のハードウェア資源を用いて該プログラムを使用することにより、既存のハードウェアで新たなアプリケーションとしての本発明の構成が容易に実行できるようになる。また該プログラムを固定する記録媒体の構成は、上記のソフトウェア商品として配布・販売する構成の他、RAMやROMなどの内部記憶装置の構成やハードディスクなどの外部記憶装置の構成も、そのようなプログラムがそこに記録されれば、該記録媒体に含まれることは言うまでもない。

【0040】そのうち、請求項19のプログラムの構成は、請求項1の構成に対応する構成であり、その具体的構成は、コンピュータに、少なくとも暗証データに対して一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データを読み取らせるステップと、入力された暗証データに対し上記と同じ一方向性関数によって第2の照合用データを算出させるステップと、該第2の照合用データと前記第1の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴としている。

【0041】請求項20のプログラムの構成は、請求項2の構成に対応する構成であり、その具体的構成は、コンピュータに、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータを読み取らせるステップと、読み取られたユーザデータと入力された暗証データを少なくとも構成要素とするデータ列に対し上記と同じ一方向性関数によって第2の照合用データを算出させるステップと、該第2の照合用データと前記第1の照合用データとを照合させ、本人確認を行うステップとを実行させることを特徴としている。

【0042】請求項21のプログラムの構成は、請求項13の構成に対応する構成であり、その具体的構成は、コンピュータに、少なくとも暗証データに対して第1の一方向性関数により処理して得られる第1の照合用データの記録された媒体から、第1の照合用データが読み取られ、入力された暗証データに対し上記第1の一方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記記憶体から、第1の照合用データ、第3の照合用データ及び上記保管情報を読み取らせるステップと、別途入力された暗証データに対し上記第1の一方向性関数によって第4の照合用データを算出させるステップと、第4の照合用データと読み取られた前記第1の照合用データとを照合させるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第5の照合用データを算出させるステップと、上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとを照合させるステップと、第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴としている。

【0043】請求項22のプログラムの構成は、請求項14の構成に対応する構成であり、その具体的構成は、コンピュータに、ユニークなユーザデータと暗証データを少なくとも構成要素とするデータ列に対して第1の一方向性関数により処理して得られる第1の照合用データ及び上記ユーザデータの記録された媒体から、第1の照合用データ及びユーザデータが読み取られ、入力された暗証データ及び上記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方向性関数によって第2の照合用データが算出された後、第2の照合用データと前記第1の照合用データとが照合されると共に、入力された前記暗証データと別途入力された任意の保管情報を少なくとも構成要素とするデータ列に対し、上記第1の一方向性関数又は第2の一方向性関数によって第3の照合用データが算出され、第2の照合用データと第1の照合用データとが一致したことにより、該保管情報と第3の照合用データとが記録されたという経緯を有する上記媒体から、ユーザデータ、第1の照合用データ、第3の照合用データ及び上記保管情報を読み取らせるステップと、別途入力された暗証データ及び読み取られた上

記ユーザデータを少なくとも構成要素とするデータ列に対し上記第1の一方方向性関数によって第4の照合用データを算出させるステップと、第4の照合用データと読み取られた前記第1の照合用データとを照合させるステップと、読み取られた保管情報と別途入力された前記暗証データを少なくとも構成要素とするデータ列に対し、上記第1の一方方向性関数又は第2の一方方向性関数によって第5の照合用データを算出させるステップと、上記照合ステップで第4の照合用データと第1の照合用データとが一致したことを条件として、読み取られた前記第3の照合用データと上記第5の照合用データとを照合させるステップと、第3の照合用データと第5の照合用データとが一致する場合に、読み取られた保管情報を処理するステップとを実行させることを特徴としている。

【0044】請求項24の構成は、上記請求項19〜請求項23のいずれかのプログラムを記録したコンピュータ読み取り可能な記録媒体について規定する。

【0045】

【発明の実施の形態】以下、本発明の実施の形態を図示例と共に説明する。

(実施例1) 図1は、本発明によって、ICカードよりなる媒体1の所有者が本人であることの確認が行えるシステムを、金融機関のATM (Automatic Teller Machine) において適用した場合の、媒体作成装置2による媒体作成工程を示す説明図である。

【0046】同図に示すように、ユーザは、カード発行側に対し、ICカード(媒体1)の発行して欲しい旨の申込を行うと、カード発行側は、該ユーザ用にユニークなユーザIDを割り当て、それをユーザ側に通知する。またカード発行側は、該ユーザに対して、該ユーザが望む暗証番号を入力するよう求め、ユーザ側からの暗証番号の通知を受け付ける。以上の工程は、ユーザ側がネットを介してカード発行側のサーバにアクセスすることで行われるが、ネットを使わず、窓口において行っても良い。

【0047】尚、上記暗証番号は、ユーザが望む適宜の数字・文字・記号などではなく、たとえば指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報などのユーザの身体的特徴を検出させて、その検出データを用いるようにしても良い。媒体1に記録される第1の照合用データは、後述するように、ハッシュ関数で処理されて得られるものであるため、解析することはできないが、暗証番号が盗用された場合は、上記媒体1乃至そのコピー品を使用する限り、本人と誤認識されてしまう可能性がある。従って、そのような盗用ができないように、該媒体1に記載される暗証番号は、ユーザの身体的特徴の検出データなどの方、他人のハッキングによるなりすましを防ぐ意味で望ましい。

【0048】ここで、媒体作成に必要なユーザIDと暗証番号が揃うので、これらが、後述する媒体作成装置2

に入力される。該媒体作成装置2は、これらの入力データに対して、ハッシュ関数処理を行い、第1の照合用データを生成する。そして該第1の照合用データを、上記ユーザIDと共に、前記媒体1に書き込む。この媒体1は、上記ユーザに交付される。

【0049】図2は、上記媒体作成装置2の機能構成を示す機能ブロック図である。同図に示すように、ユーザIDと暗証番号のデータ列が与えられることによりハッシュ関数で処理して第1の照合用データを算出する演算手段21と、該第1の照合用データを媒体1に書き込む書込手段22とを有している。

【0050】このような構成により本人確認用に上記媒体1が作成されるので、できあがった媒体1には、ユーザIDと第1の照合用データが記録されるのみで、暗証番号そのものはない。しかも第1の照合用データは、逆方向の解析が不能な(一方方向性の)ハッシュ関数で処理されており、該第1の照合用データからは、暗証番号などを割り出すことはできない。さらに元となったデータには、ユーザIDが含まれており、それ自身はユニークなデータであるため、生成された第1の照合用データもユニークなものとなり、他人のものと同一になることはない。

【0051】図3は、ユーザが上記媒体1を使用して、本人確認を行う場合に使用される本人確認装置3における本人確認処理の工程説明図である。この場合の本人確認装置3は、金融機関における上記ATMで構成されることになる。

【0052】同図に示すように、ユーザは、本人確認装置3の挿入口に上記媒体1を挿入する。すると暗証番号の入力が求められるので、暗証番号の入力を行う。ここでは、媒体1の作成時の状態に応じて、ユーザの身体的特徴をセンサなどで検出させ、その検出データを暗証番号として入力することもできる。

【0053】ここで、本人確認の際に第2の照合用データ生成に必要なユーザID(媒体1より読み込まれる)と暗証番号(ユーザによる入力)が揃うので、これらのデータに対して、上記と同一のハッシュ関数を用いた処理が行われ、第2の照合用データが生成される。そして媒体1より読み込まれた第1の照合用データと生成された該第2の照合用データとの照合が行われる。これらのデータが一致すれば、媒体1の所有者が該ユーザであると確認され(本人確認がなされ)、該本人確認装置3が組み込まれているATMにおけるその他の操作が許可され、以後ユーザによって、ATMにおける任意の操作が実施される。

【0054】図4は、上記本人確認装置3の機能構成を示す機能ブロック図である。同図に示すように、上記媒体1から、第1の照合用データ及びユーザIDを読み取る照合用データ読み取り手段31と、テンキーやタッチパネル(或いはユーザの身体的特徴を検出するセンサ)

などで構成される暗証番号の入力手段32と、読み取られたユーザIDと入力された暗証番号のデータ列に対し上記と同じハッシュ関数によって第2の照合用データを算出する算出手段33と、生成された第2の照合用データと読み取られた第1の照合用データとを照合する照合手段34と、照合結果に基づき、本人か否かの判定を行う判定手段35とを有している。

【0055】上記構成によれば、媒体1からは上述のように、暗証番号の割り出しはできないので、本人確認を行う際に、媒体1の所持人に対し、入力手段32からの暗証番号の入力を要求し、入力された暗証番号及び読み取られたユーザIDに対して、算出手段33により上記と同一のハッシュ関数で処理し、その結果得られた第2の照合用データと、前記媒体1より読み取られた第1の照合用データとが、照合手段34で突き合わされ、判定手段35により、本人確認が行われるので、他の装置との接続が要求されることなく媒体1単体で、媒体1の所持人が、ユーザ本人であると確認することができるようになる。しかも媒体1に格納されるデータは、上述のように、本人確認のために入力されるべき暗証番号そのもののデータではなく、しかも媒体1上に格納されるデータからは、入力の要求される暗証番号の割り出しが困難なため、セキュリティも向上することになる。

【0056】図5は、上記媒体作成装置2における処理の手順を示すフローチャートである。同図に示すように、ユーザ側からのアクセスで、媒体1の発行の申込があると、該媒体作成装置2により、該ユーザに対するユーザIDが決定され、該ユーザIDが、このユーザに通知される(ステップS101)。そして通知済か否かの確認がなされ(ステップS102)、通知していなければ(ステップS102; No)、ステップS101に復帰する。

【0057】通知済であれば(ステップS102; Yes)、ユーザの希望する暗証番号の入力(ユーザの身体的特徴を検出させる場合もある)を促す表示がなされ(ステップS103)、暗証番号が入力されたか否かがチェックされる(ステップS104)。該暗証番号の入力がなければ(ステップS104; No)、前記ステップS103に復帰する。

【0058】上記ユーザIDと入力された暗証番号を基にハッシュ関数処理がなされ、第1の照合用データが生成される(ステップS105)。

【0059】生成された第1の照合用データが存在するかがチェックされ(ステップS106)、該データがなければ(ステップS106; No)、前記ステップS105に復帰する。

【0060】上記第1の照合用データが確認されれば(ステップS106; Yes)、媒体1に当該データ及びユーザIDの書き込みがなされる(ステップS107)。そして該媒体1上に第1の照合用データ及びユー

ザIDがあるか否かが確認される(ステップS108)。

【0061】媒体1上に第1の照合用データ及びユーザIDが無ければ(ステップS108; No)、前記ステップS107に復帰する。反対に媒体1上にこれらのデータがあれば(ステップS108; Yes)、処理を終了する。そしてこの媒体1がユーザに交付される。

【0062】図6は、上記本人確認装置3における処理の手順を示すフローチャートである。同図に示すように、ATM上の本人確認装置3では、挿入口における媒体1の挿入が検出され(ステップS201)、該媒体1が挿入されたか否かがチェックされる(ステップS202)。媒体1の挿入が検出されない場合(ステップS202; No)、前記ステップS201に戻る。

【0063】媒体1の挿入が検出されれば(ステップS202; Yes)、該媒体1からのユーザID及び第1の照合用データの読み取りがなされる(ステップS203)。そしてこれらのデータが読み取られたか否かがチェックされる(ステップS204)。読み取りが完了していなければ(ステップS204; No)、前記ステップS201に復帰する。

【0064】上記データの読み取りが完了していれば(ステップS204; Yes)、ユーザの暗証番号の入力(ユーザの身体的特徴を検出させる場合もある)を促す表示がなされ(ステップS205)、暗証番号が入力されたか否かがチェックされる(ステップS206)。該暗証番号の入力がなければ(ステップS206; No)、前記ステップS205に戻る。

【0065】上記暗証番号の入力があった場合(ステップS206; Yes)、読み取られた上記ユーザIDと入力された暗証番号を基にハッシュ関数処理がなされ、第2の照合用データが生成される(ステップS207)。

【0066】生成された第2の照合用データが存在するかがチェックされ(ステップS208)、該データがなければ(ステップS208; No)、前記ステップS207に復帰する。

【0067】上記第2の照合用データが確認されれば(ステップS208; Yes)、両照合用データの照合がなされる(ステップS209)。その照合結果で、両データが一致するか否かがチェックされ(ステップS210)、一致しなければ(ステップS210; No)、前記ステップS205に復帰する。

【0068】反対に両データが一致する場合(ステップS210; Yes)、本人確認ができたとして(ステップS211)、該本人確認装置3における処理は終了し、入出金処理、振込・振り替え処理、照会処理など、種々の前記ATMにおける操作が可能になる。

【0069】上記実施例構成によれば、媒体1中に格納されるデータは、暗証番号そのものではなく、ハッシュ

関数により処理して得られる第1の照合用データであり、そのため、仮に媒体1からこれらのデータが読み出せたとして、第1の照合用データからは、暗証番号を割り出すことはできない。従って本人確認の際に暗証番号の入力（場合によりユーザの身体的特徴の検出）を要求することで、入力された暗証番号に対し上記と同一のハッシュ関数で処理し、その結果得られた第2の照合用データと、前記媒体1より読み取った第1の照合用データとの突き合わせを行い、その照合結果で本人確認処理を行えば、他の装置との接続が要求されることなく、該媒体1だけで本人確認が完結できることになる。また媒体1上に格納されるデータは、本人確認のために入力される暗証番号そのものではなく、しかも媒体1上に格納されるデータからは、上記入力の要求される暗証番号の割り出しが困難なため、セキュリティも向上することになる。すなわち、ユーザ以外は、いかなる者も真の暗証番号を目にすることなく安全に媒体1が作成され、媒体1の盗難、偽造などに対しても、極めて強力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体1作成中の暗証番号の盗難リスクなども回避されるようになる。

【0070】（実施例2）図7～図12は、本発明によって、ICカードよりなる媒体1の所有者が、例えば金融機関のATMに備えられた後述する保管情報処理装置5において実行される処理シーケンスや該装置5において実行できるソフトウェアなどの自己の希望する情報を予め該媒体1に登録しておき、該保管情報処理装置5で上記所有者がユーザ本人であると確認された際に、それらの情報の処理が行われるシステムを説明したものであり、そのうち特に図7は、媒体作成装置2による媒体作成工程を示す説明図である。

【0071】実施例1と同様、ユーザは、カード発行側に対し、ICカード（媒体1）の発行して欲しい旨の申込を行うと、カード発行側は、該ユーザ用にユニークなユーザIDを割り当て、それをユーザ側に通知する。またカード発行側は、該ユーザに対して、該ユーザが望む暗証番号を入力するよう求め、ユーザ側からの暗証番号の通知を受け付ける。以上の工程は、ユーザ側がネットを介してカード発行側のサーバにアクセスすることで行われるが、ネットを使わず、窓口において行っても良い。

【0072】また、本実施例構成においても、上記暗証番号は、ユーザが望む適宜の数字・文字・記号などではなく、たとえば指紋、眼球の光彩部分の特徴、腕等に浮き出ている血管の位置情報などのユーザの身体的特徴を検出させて、その検出データを用いるようにしても良い。

【0073】ここで、媒体作成に必要なユーザIDと暗証番号が揃うので、これらが、媒体作成装置2に入力さ

れる。該媒体作成装置2は、これらの入力データに対して、第1のハッシュ関数を用いた処理を行い、第1の照合用データを生成する。そして該第1の照合用データを、上記ユーザIDと共に、前記媒体1に書き込む。この媒体1は、上記ユーザに交付される。

【0074】上記媒体作成装置2は、前記実施例1の構成と同じであるので、ここではその説明は省略する。

【0075】このような構成により本人確認用に上記媒体1が作成されるので、できあがった媒体1には、ユーザIDと第1の照合用データが記録されるのみで、暗証番号そのものはない。しかも第1の照合用データは、逆方向の解析が不能な第1のハッシュ関数で処理されており、該第1の照合用データからは、暗証番号などを割り出すことはできない。さらに元となったデータには、ユーザIDが含まれており、それ自身はユニークなデータであるため、生成された第1の照合用データもユニークなものとなり、他人のものと同一になることはない。

【0076】図8は、後述する保管情報処理装置5において実行される処理シーケンスや該装置5において実行できるソフトウェアなどのユーザ自身が望む情報を、交付された媒体1に、予め登録しておくための情報保管装置4の構成説明図である。

【0077】該情報保管装置4は、前記図7で示したように、カード発行側から貸与された情報保管ソフトウェアのインストールされたユーザ側のパソコンと、媒体1の情報を読み書きするために該パソコンに接続されたカードリーダーからなるデータ読取書込手段41とで構成されている。尚、上記情報保管ソフトウェア中に規定される第1のハッシュ関数（第1の算出手段43で使用）は、上記媒体作成装置2及び後述する保管情報処理装置5において夫々第1の照合用データ及び第4の照合用データ生成時に使用されるハッシュ関数と同一のものであり、また同じく上記情報保管ソフトウェア中に規定される第2のハッシュ関数（第2の算出手段46で使用）は、保管情報処理装置5において第5の照合用データ生成時に使用されるハッシュ関数と同一のものである。

【0078】ユーザは、この情報保管装置4を使用して、自分の望む情報を、交付された媒体1に予め登録しておくことができるようになる。ここで登録しておくことのできる情報とは、上述のように、後述する保管情報処理装置5（本実施例では、特定カード向けに該カード上にユーザの規定する処理の実行ができるようにした、JAVA、MULTOS、WINDOWSなどの汎用OSの稼働するATM）で実行することが予定される複数処理の連続実行シーケンスや該装置5において実行できるソフトウェアなどがある。

【0079】図9は、上記情報保管装置4の機能構成を示す機能ブロック図である。同図に示すように、上記媒体1から、第1の照合用データ及びユーザIDを読み取

り、後に、算出手段46によって算出された第3の照合用データ及び保管情報を媒体1に書き込むことができるデータ読取書込手段41と、テンキーやタッチパネル（或いはユーザの身体的特徴を検出するセンサ）などで構成される暗証番号の入力手段42と、読み取られたユーザIDと入力された暗証番号のデータ列に対して、媒体作成装置2と同じ第1のハッシュ関数によって第2の照合用データを算出する第1の算出手段43と、生成された第2の照合用データと読み取られた第1の照合用データとを照合する照合手段44と、照合結果に基づき、本人か否かの判定を行う判定手段45と、本人であると判定された場合に、ユーザのパソコン内の記憶装置（ハードディスクなど）に記録された或いはキーボードなどから入力される上記保管情報と入力された上記暗証番号を基に、第2のハッシュ関数によって第3の照合用データを算出する第2の算出手段46とを有している。

【0080】上記情報保管装置4は、ユーザがパソコン上で情報保管ソフトウェアを起動させることで構成される。そして、ユーザが、ユーザID及び第1の照合用データの記録された上記媒体1をデータ読取書込手段41に挿入し、該媒体1から、ユーザID及び第1の照合用データを読み取らせる。すると、暗証番号の入力が求められるので、ユーザはこれを入力する（又はセンサに身体的特徴を検出させる）。入力（又は検出）された暗証番号と読み取られたユーザIDを基に、第1の算出手段43により、第1のハッシュ関数を使用した処理がなされ、第2の照合用データが生成される。生成された第2の照合用データと読み取られた前記第1の照合用データとが、照合手段44により照合される。その照合結果が判定手段45で判定され、両データが一致すれば、該媒体1の所有者がユーザであると判定される。そして上記記憶装置或いはキーボードなどから入力された上記保管情報と入力（又は検出）された前記暗証番号とからなるデータ列を基に、第2の算出手段46により、第2のハッシュ関数を用いた処理がなされ、第3の照合用データが生成される。生成された第3の照合用データと前記保管情報とが、前記データ読取書込手段41により、媒体1に書き込まれる。

【0081】図10は、上記保管情報処理装置5の機能構成を示す機能ブロック図である。同図に示すように、保管情報処理装置5の構成は、上記媒体1から、ユーザID、第1の照合用データ、第3の照合用データ及び上記保管情報を読み取るデータ読み取り手段51と、テンキーやタッチパネル（或いはユーザの身体的特徴を検出するセンサ）などで構成される暗証番号の入力手段52と、読み取られたユーザIDと入力された暗証番号のデータ列に対して、媒体作成装置2及び情報保管装置4と同じ第1のハッシュ関数によって第4の照合用データを算出する第1の算出手段53と、生成された第4の照合用データと読み取られた第1の照合用データとを照合す

る第1の照合手段54と、照合結果に基づき、本人か否かの判定を行う第1の判定手段55と、その媒体所有者が本人であると判定された場合に、読み取られた保管情報と入力された暗証番号のデータ列に対して、前記情報保管装置4と同じ第2のハッシュ関数によって第5の照合用データを算出する第2の算出手段56と、生成された第5の照合用データと読み取られた第3の照合用データとを照合する第2の照合手段57と、照合結果に基づき、保管情報の内容に改竄がないか否かの判定を行う第2の判定手段58と、保管情報の内容に改竄がないと判定された場合に、保管情報の処理を行う処理手段59とを有している。

【0082】図11は、上記のようにしてユーザに保管情報の書き込みが行われた媒体1を使用して、該ユーザが、金融機関のATM上で当該保管情報を実行させることを可能にする保管情報処理装置5における処理の工程説明図である。この場合の保管情報処理装置5は、金融機関における上記ATMで構成されることになる。

【0083】同図に示すように、ユーザは、保管情報処理装置5の挿入口に上記媒体1を挿入する。すると暗証番号の入力が求められるので、暗証番号の入力を行う。ここでは、媒体1の作成時の状態に応じて、ユーザの身体的特徴をセンサなどで検出させ、その検出データを暗証番号として入力することもできる。

【0084】ここで、本人確認の際に第4の照合用データ生成に必要なユーザID（媒体1より読み込まれる）と暗証番号（ユーザによる入力）が揃うので、これらのデータに対して、上記と同一の第1のハッシュ関数を用いた処理が行われ、第4の照合用データが生成される。そして媒体1より読み込まれた第1の照合用データと生成された該第4の照合用データとの照合が行われる。これらのデータが一致すれば、媒体1の所有者が該ユーザであると確認される（本人確認がなされる）。

【0085】本人確認がなされると、読み出された保管情報と入力された前記暗証番号に対して、情報保管装置4で用いられたと同一の第2のハッシュ関数を用いた処理が行われ、第5の照合用データが生成される。そして媒体1より読み込まれた第3の照合用データと生成された該第5の照合用データとの照合が行われる。これらのデータが一致すれば、媒体1に保管されている情報には改竄がないと判断される（不正アクセスがないと判断される）。その後上記ATM上で、該保管情報の処理がなされる。

【0086】図12は、上記保管情報処理装置5における処理の手順を示すフローチャートである。同図に示すように、ATM上の保管情報処理装置5では、挿入口における媒体1の挿入が検出され（ステップS301）、該媒体1が挿入されたか否かがチェックされる（ステップS302）。媒体1の挿入が検出されない場合（ステップS302；No）、前記ステップS301に戻る。

【0087】媒体1の挿入が検出されれば（ステップS302；Yes）、該媒体1からのユーザID、第1及び第3の照合用データ並びに保管情報の読み取りがなされる（ステップS303）。そしてこれらのデータが読み取られたか否かがチェックされる（ステップS304）。読み取りが完了していなければ（ステップS304；No）、前記ステップS301に復帰する。

【0088】上記データの読み取りが完了していれば（ステップS304；Yes）、ユーザの暗証番号の入力（ユーザの身体的特徴を検出させる場合もある）を促す表示がなされ（ステップS305）、暗証番号が入力されたか否かがチェックされる（ステップS306）。該暗証番号の入力がなければ（ステップS306；No）、前記ステップS305に戻る。

【0089】上記暗証番号の入力があつた場合（ステップS306；Yes）、読み取られた上記ユーザIDと入力された暗証番号を基に第1のハッシュ関数による処理がなされ、第4の照合用データが生成される（ステップS307）。

【0090】生成された第4の照合用データが存在するかがチェックされ（ステップS308）、該データがなければ（ステップS308；No）、前記ステップS307に復帰する。

【0091】上記第4の照合用データが確認されれば（ステップS308；Yes）、読み取られた第1の照合用データと生成された第4の照合用データとの照合がなされる（ステップS309）。その照合結果で、両データが一致するか否かがチェックされ（ステップS310）、一致しなければ（ステップS310；No）、前記ステップS305に復帰する。

【0092】反対に両データが一致する場合（ステップS310；Yes）、本人確認ができたとして、読み取られた保管情報と入力された暗証番号を基に第2のハッシュ関数による処理がなされ、第5の照合用データが生成される（ステップS311）。

【0093】生成された第5の照合用データが存在するかがチェックされ（ステップS312）、該データがなければ（ステップS312；No）、前記ステップS311に復帰する。

【0094】上記第5の照合用データが確認されれば（ステップS312；Yes）、読み取られた第3の照合用データと生成された第5の照合用データとの照合がなされる（ステップS313）。その照合結果で、両データが一致するか否かがチェックされ（ステップS314）、一致しなければ（ステップS314；No）、保管情報の処理がなされない旨表示し、該処理を拒否する（ステップS316）。

【0095】反対に両データが一致する場合（ステップS314；Yes）、上記保管情報に従った処理（その保管情報の内容に応じた入出金処理、振込・振り替え処

理、照会処理などの処理）が、該ATM上で実行される（ステップS315）。

【0096】上記実施例構成によれば、媒体1の所有者がユーザ本人であることの確認ができると同時に、該媒体1から、ユーザによって記録された任意の保管情報を取り出して利用することができ、しかもその利用時に、利用者が媒体1の正しい所有者又は媒体1に上記保管情報を記録した者であることの照合がなされ、さらに記録された保管情報に改竄がないことの確認が行えるようになる。

【0097】尚、本発明の本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体は、上述の実施例にのみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【0098】

【発明の効果】以上、説明したように本発明の請求項1～請求項24記載の本人確認方法、本人確認装置、媒体作成装置、媒体、媒体保管情報の処理方法、プログラム及び記録媒体によれば、他の装置との接続が要求されることなく、媒体の記録内容を読み取らせるだけで本人確認ができるようになると共に、上記媒体上に格納されるデータは、本人確認のために入力されるデータそのものではなく、しかも該媒体上に格納されるデータからは、上記入力の要求される本人確認のためのデータの割り出しが困難なため、セキュリティも向上することになるという優れた効果を奏し得る。そのため、媒体の盗難、偽造などに対しても、極めて強力に対抗できるセキュリティを提供することができるようになり、さらに郵送中や媒体発行者の業務遂行中、或いは媒体作成中の暗証番号の盗難リスクなども回避されるようになる。

【0099】さらに請求項13～請求項18、及び請求項21～請求項24までに記載の構成によれば、媒体の所有者が本人であることの確認ができると同時に、該媒体から、本人によって記録された任意の保管情報を取り出して利用することができ、しかもその利用時に、利用者が媒体の正しい所有者又は媒体に上記保管情報を記録した者であることの照合がなされ、さらに記録された保管情報に改竄がないことの確認が行えるようになるので、媒体に保管された情報についての信頼性を確保しながら、該保管情報による機器の操作の自動実行などの処理（上記保管情報に規定された処理）ができるようになる。

【図面の簡単な説明】

【図1】媒体作成装置2による媒体作成工程を示す説明図である。

【図2】媒体作成装置2の機能構成を示す機能ブロック図である。

【図3】本人確認装置3における本人確認処理の工程説明図である。

【図4】本人確認装置3の機能構成を示す機能ブロック図である。

【図5】媒体作成装置2における処理の手順を示すフローチャートである。

【図6】本人確認装置3における処理の手順を示すフローチャートである。

【図7】媒体作成装置2による媒体作成工程を示す説明図である。

【図8】情報保管装置4の構成説明図である。

【図9】情報保管装置4の機能構成を示す機能ブロック図である。

【図10】保管情報処理装置5の機能構成を示す機能ブロック図である。

【図11】保管情報処理装置5における処理の工程説明図である。

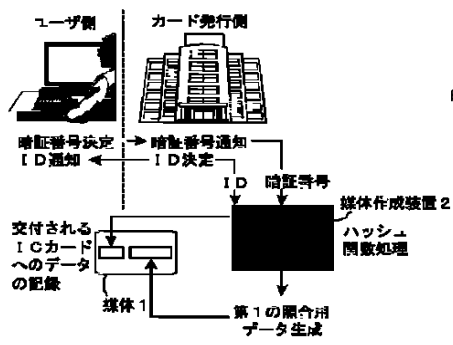
【図12】保管情報処理装置5における処理の手順を示すフローチャートである。

【符号の説明】

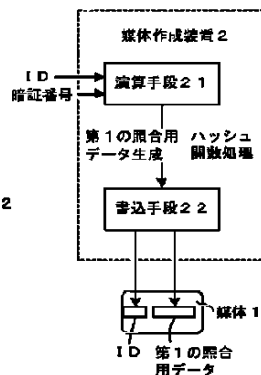
- |   |          |
|---|----------|
| 1 | 媒体       |
| 2 | 媒体作成装置   |
| 3 | 本人確認装置   |
| 4 | 情報保管装置   |
| 5 | 保管情報処理装置 |

- |    |            |
|----|------------|
| 21 | 演算手段       |
| 22 | 書込手段       |
| 31 | 照合用データ読取手段 |
| 32 | 入力手段       |
| 33 | 算出手段       |
| 34 | 照合手段       |
| 35 | 判定手段       |
| 41 | データ読取書込手段  |
| 42 | 入力手段       |
| 43 | 第1の算出手段    |
| 44 | 照合手段       |
| 45 | 判定手段       |
| 46 | 第2の算出手段    |
| 51 | データ読取手段    |
| 52 | 入力手段       |
| 53 | 第1の算出手段    |
| 54 | 第1の照合手段    |
| 55 | 第1の判定手段    |
| 56 | 第2の算出手段    |
| 57 | 第2の照合手段    |
| 58 | 第2の判定手段    |
| 59 | 処理手段       |

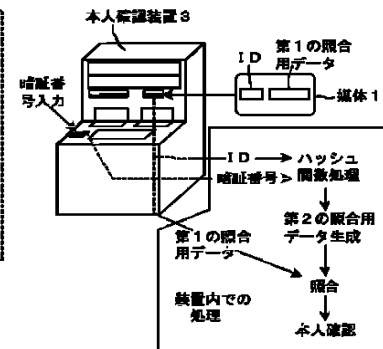
【図1】



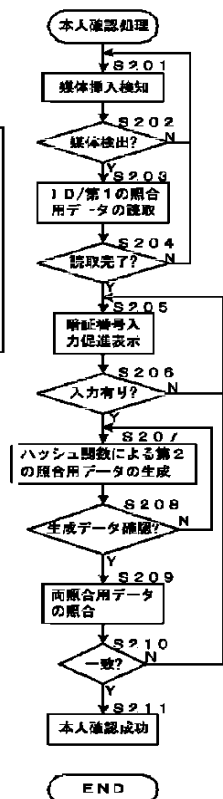
【図2】



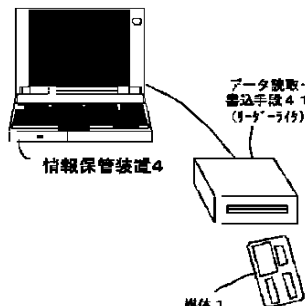
【図3】



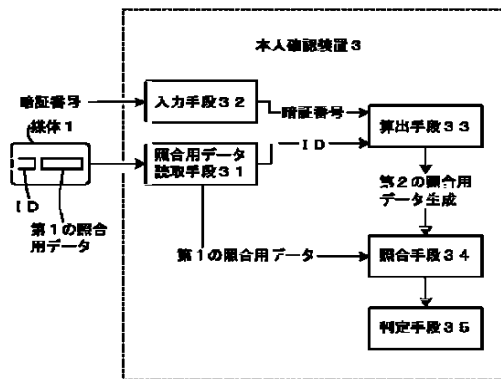
【図6】



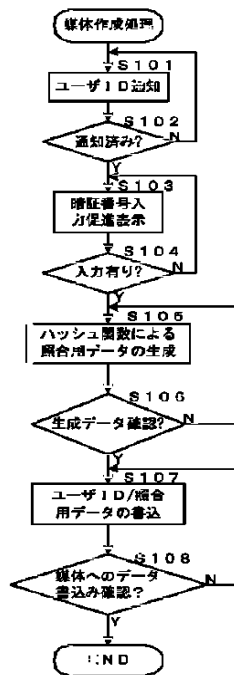
【図8】



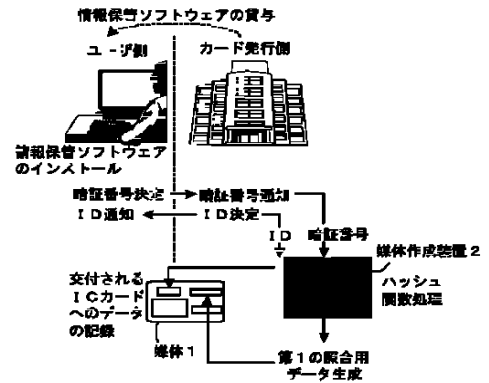
【図4】



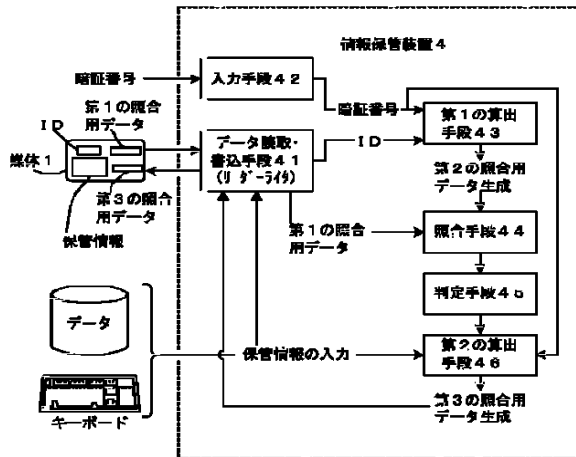
【図5】



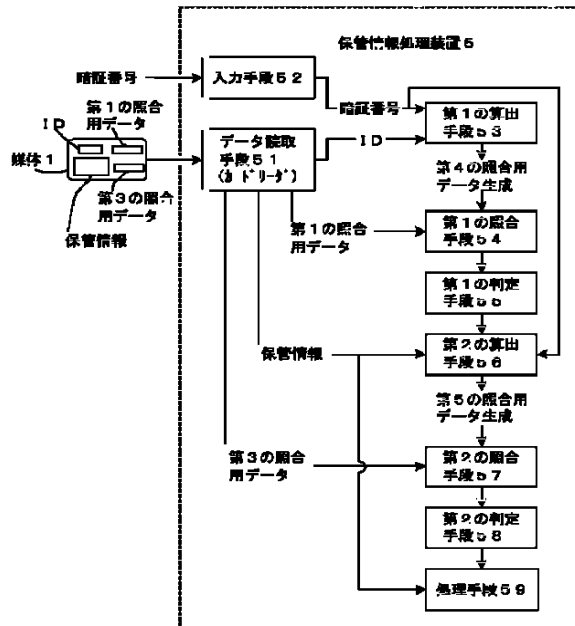
【図7】



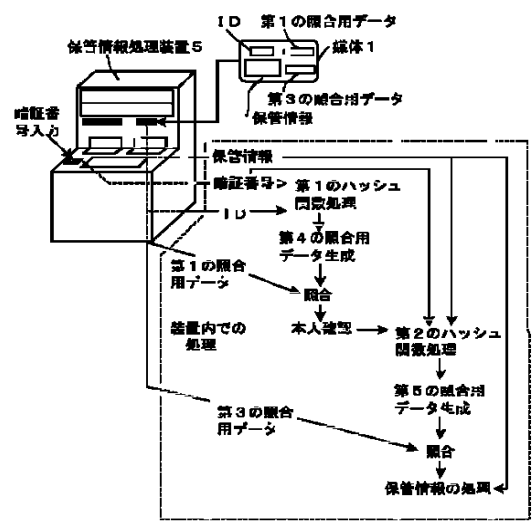
【図9】



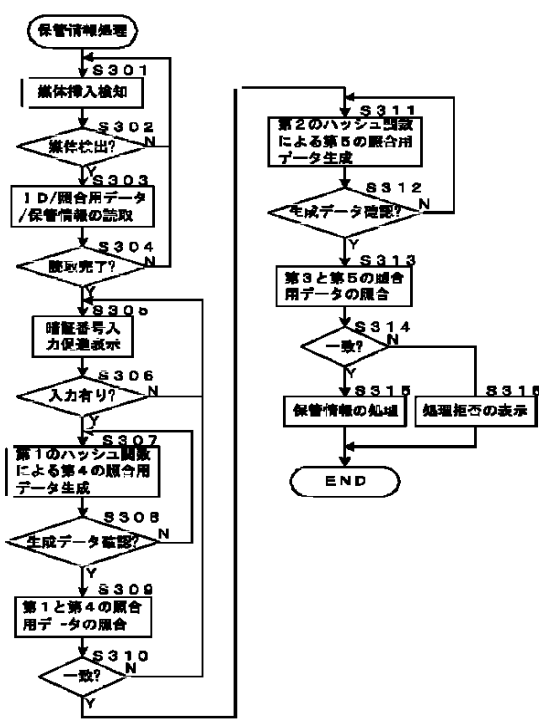
【図10】



【図11】



【図12】



フロントページの続き

(51)Int.Cl. <sup>7</sup>	識別記号	F I	(参考)
G 0 6 F 17/60	2 2 2	G 0 6 F 17/60	2 2 4
	2 2 4	G 0 9 C 1/00	6 4 0 A
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 7 5 A

Fターム(参考) 2C005 HA03 HB09 HB20 JA01 JA11  
MA04 MB08 NB01 SA07 SA12  
SA13  
5B085 AE02 AE03 AE09  
5J104 AA07 AA16 EA03 EA08 KA01  
KA03 NA05 NA11 NA12 NA34  
NA35 PA12